18/5/3 (Item 2 from file: 35)
DIALOG(R)File 35: Dissertation Abs Online

01704496 ORDER NO: AAD99-29347
DYNAMIC MANAGEMENT OF COMPUTATION AND COMMUNICATION RESOURCES TO ENABLE SECURE HIGH-PERFORMANCE APPLICATIONS (DYNAMIC RESOURCE ALLOCATION, ADAPTIVE SECURITY, RISK ASSESSMENT, INTERNET)

Author: SCHNECK, PHYLLIS ADELE
Degree: PH.D.
Year: 1998
Corporate Source/Institution: GEORGIA INSTITUTE OF TECHNOLOGY (0078)
Advisor: KARSTEN SCHWAN
Source: Volume 6005B of Dissertations Abstracts International.
PAGE 2218 . 225 PAGES
Descriptors: COMPUTER SCIENCE
Descriptor Codes: 0984

Current Internet usage for commercial applications is increasing exponentially. Electronic commerce trends are demanding greater security for network-enabled collaboration as well as business transactions that use Virtual Private Networks (public networks supporting communication between private hosts). Security measures are also necessary to enable applications for network rating standards, law enforcement, air traffic control, and wireless communications. Thus, the growth of commercial electronic communication demands a growth in security provision. Augmenting traditional data transport with security measures performed at end hosts can potentially degrade the performance of networked applications, creating an inherent security vs. performance tradeoff.

This thesis addresses this tradeoff by adapting to current system loads and security requirements to provide adaptive security through **dynamic** resource allocation. This work targets multi-stream, networked collaborative applications running on heterogeneous, unstructured distributed computing platforms that resemble subsections of the Internet. The goal is to minimize security risk by enabling CPU and network resources to be available and dynamically applied to security operations as needed for application streams to vary their security levels.

As the demand for network-based applications grows, the instances of changes in end-host connection requirements increase. Systems must have the capability to dynamically adapt security provision to changing requirements of hosts, networks, and applications. To address this need, this thesis presents a framework which incorporates admission control and run-time adaptive methods for per-stream security resource contracts within which these issues are addressed. This work comprises the following contributions: (1) formulation of new metrics to quantify performance and security; (2) formulation of rational mapping of user-requested security level to CPU resources; (3) formulation of heuristics for dynamically **altering security level** based on current resource allocation

(patent pending); (4) formulation of the concept of risk as it applies to adaptive security; (5) formulation of joint optimization of computation resources for overall risk minimization; and (6) application of the mapping of security level to CPU and network resources to enable: (a) global tracking of resource availabilities of all registered end-hosts, (b) criticality-based risk management, and (c) on-line global optimization to minimize &ldquo;exposure&rdquo; for a system of multiple application connections between multiple hosts.

Dialog eLink: Check for PDF Download Availability and Purchase
18/5/11 (Item 2 from file: 6)
DIALOG(R)File 6: NTIS

2237040 **NTIS Accession Number:** ADA401378/XAB
Dynamic Parameterization of IPSEC
(Master's thesis)
Agar, C. D.
Naval Postgraduate School, Monterey, CA.
Corporate Source Codes: 019895000; 251450

Dec 2001 334p
Language: English Document Type: Thesis
Journal Announcement: USGRDR0219
The original document contains color images.
Hard copy only. Product reproduced from digital image. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)605-6900; and email at orders@ntis.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A16/MF A03
Country of Publication: United States

The Internet has become the medium of choice for communications between most Government and Military organizations. Unfortunately the key Internet protocols were not designed to provide security and their security vulnerabilities have become apparent. IPsec was developed to provide users with a range of security services, for both confidentiality and integrity, enabling them to securely pass information across networks. Automated security mechanisms are typically designed and/or calibrated to meet an organization's security policy. However, once the mechanism in operation the implemented policy is in a static state, and cannot be adjusted according to **dynamic** environmental conditions. This means that security mechanisms fail to reflect the policy that is appropriate for the **changing** contexts. **Dynamic** parameterization enables **security** mechanisms to **adjust** the **level** of **security** service '**on**-the-**fly**' to respond to changing conditions (i.e., INFOCON, THREATCON). This work includes the extension of the attributes encoded by the KeyNote Trust Management System and modification of the IPsec mechanism to incorporate **dynamic** parameters into the security service selection mechanism, and the construction of a graphical user interface, for demonstrating 'proof-of-concept' of **Dynamic** Parameterization of OpenBSD 2.8 IPsec.

Descriptors: *Information security; Policies; Automation; Management planning and control; Vulnerability; Theses; Internet; Military organizations; Graphical user interface
Identifiers: Sad(Security association database); Sa(Security association); Spd(Security policy database); NTISDODXA
Section Headings: 62GE (Computers, Control, and Information Theory--General)

12/3,K/1 (Item 1 from file: 610) **[bad date]**
DIALOG(R)File 610: Business Wire

00784736 20021001274B0964 **(USE FORMAT 7 FOR FULLTEXT)**
Rappore Technologies Begins Shipping Rappore Shield v1.1 -- Location-Aware Software Keeps Wireless Computer Users Secure-Rappore Shield Automatically Adapts Security Protections Based on Location

Business Wire
Tuesday , October 1, 2002 11:03 EDT
Journal Code: BW **Language:** ENGLISH **Record Type:** FULLTEXT **Document Type:** NEWSWIRE
Word Count: 708

Text:

...office wirelessly connected to a LAN behind
the corporate firewall.

Rappore Shield v1.1 automatically **changes security settings** for wireless
access when **laptop** users **move** from work to home or from home
to an
"on-the-road" location. At the...

Dialog eLink: Order File History
18/9/8 (Item 5 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0013332934 *Drawing available*
WPI Acc no: 2003-420365/200339
XRPX Acc No: N2003-335741
Security management apparatus for portable personal computer, includes control unit for changing security level based on position of portable personal computer which is detected by position detector
Patent Assignee: FUJITSU LTD (FUIT); KIHARA M (KIHA-I); MIZUTANI K (MIZU-I); ONO S (ONOS-I); OURA S (OURA-I); SAITO M (SAIT-I)
Inventor: KIHARA M; MIZUTANI K; MIZUTANI Y; ONO J; ONO S; OURA S; SAITO M

Patent Family (2 patents, 2 countries)							
Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
US 20030061166	A1	20030327	US 200257865	A	20020129	200339	B
JP 2003099400	A	20030404	JP 2001293132	A	20010926	200339	E

Priority Applications (no., kind, date): JP 2001293132 A 20010926

Patent Details					
Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	**Filing Notes**
US 20030061166	A1	EN	14	10	
JP 2003099400	A	JA	11		

Alerting Abstract US A1
NOVELTY - The security management apparatus includes an input/output control unit for **changing security level** of a portable personal computer (PC) into one of the **security levels** which are stored in a **security** information **table**. The **security level** of the portable personal computer is changed based on the position of the portable PC which is detected by a position detector.

DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

1. security management method;
2. security management program;
3. security control program;
4. recorded medium storing security management program; and
5. security level editing program.

USE - For managing security of portable personal computer.

ADVANTAGE - Reduces user's work of rebooting the operating system (OS), hence saves time. Improves security function by changing user's authority to boot an OS based on the geographical position.

Original Abstract:
A security management apparatus, a security management method and a security management program are provided which are capable of performing access control to files, folders, etc., according to a current position of a prescribed device such as a portable terminal to be managed, In order to perform security control on a portable terminal, etc., security levels of the portable terminal are stored in advance in a predetermined table in association with the positions of the portable terminal. The current position of the portable terminal is detected by means of a GPS or the like, and a security level corresponding to the current position of the portable terminal detected is acquired from the predetermined table, so that booting of programs and/or access control to files, folders, etc., in the portable terminal are carried out based on the security level thus acquired.

Claim:
What is claimed is:

1. **1**. A security management apparatus for managing the security of a prescribed device, said apparatus comprising: a position detecting section detecting a position of said prescribed device; and a control unit changing a security level of said prescribed device according to the position of said prescribed device detected by said position detecting section.